



VSphere Metro Storage Cluster con ONTAP

Enterprise applications

NetApp
February 10, 2026

This PDF was generated from https://docs.netapp.com/it-it/ontap-apps-dbs/vmware/vmware_vmisc_overview.html on February 10, 2026. Always check docs.netapp.com for the latest.

Sommario

VSphere Metro Storage Cluster con ONTAP	1
VSphere Metro Storage Cluster con ONTAP	1
Soluzioni di disponibilità continua per ambienti vSphere	1
Che cos'è vSphere Metro Storage Cluster?	2
Panoramica della soluzione VMware vSphere	4
Alta disponibilità vSphere	5
Rilevamento errori host	5
Risposta di isolamento dell'host	6
Protezione dei componenti VM (VMCP)	6
Implementazione di VMware DRS per NetApp SnapMirror Active Sync	7
Implementazione VMware DRS per NetApp MetroCluster	7
Implementazione di VMware Storage DRS con NetApp MetroCluster	8
Linee guida per la progettazione e l'implementazione di vMSC	9
Configurazione dello storage NetApp	9
Utilizzo del plug-in vCenter di ONTAP Tools per SnapMirror Active Sync	10
Configurazione di VMware vSphere	10
Crea cluster di datastore se necessario	18
Resilienza per eventi pianificati e non pianificati	20
Scenari di errore per vMSC con MetroCluster	20
Errore singolo percorso di storage	21
Errore host ESXi singolo	21
Isolamento dell'host ESXi	23
Guasto a shelf di dischi	23
Guasto a un singolo storage controller	24
Errori del collegamento interswitch	25

VSphere Metro Storage Cluster con ONTAP

VSphere Metro Storage Cluster con ONTAP

L'hypervisor vSphere leader del settore di VMware può essere implementato come cluster stretched indicato come vSphere Metro Storage Cluster (vMSC).

Le soluzioni vMSC sono supportate sia con NetApp® MetroCluster™ che con SnapMirror Active Sync (precedentemente noto come SnapMirror Business Continuity o SMBC) e forniscono una business continuity avanzata se uno o più domini di errore subiscono un'interruzione totale. La resilienza alle diverse modalità di errore dipende dalle opzioni di configurazione scelte.



Questa documentazione sostituisce i report tecnici precedentemente pubblicati *TR-4128: VSphere on NetApp MetroCluster*

Soluzioni di disponibilità continua per ambienti vSphere

L'architettura ONTAP è una piattaforma di archiviazione flessibile e scalabile che fornisce servizi SAN (FCP, iSCSI e NVMe-oF) e NAS (NFS v3 e v4.1) per gli archivi dati. I sistemi di storage NetApp AFF, ASA e FAS utilizzano il sistema operativo ONTAP per offrire protocolli aggiuntivi per l'accesso allo storage guest, come S3 e SMB/CIFS.

NetApp MetroCluster utilizza la funzione di ha (failover del controller o CFO) di NetApp per la protezione dai guasti dei controller. Include inoltre la tecnologia SyncMirror locale, il failover cluster in caso di disastro (Cluster failover on Disaster o CFOD), la ridondanza hardware e la separazione geografica per ottenere livelli elevati di disponibilità. SyncMirror esegue il mirroring sincrono dei dati tra le due metà della configurazione MetroCluster scrivendo i dati su due plessi: Il plesso locale (sullo shelf locale) fornendo attivamente i dati e il plesso remoto (sullo shelf remoto) normalmente non fornendo i dati. La ridondanza hardware viene implementata per tutti i componenti MetroCluster, come controller, storage, cavi, switch (utilizzati con Fabric MetroCluster) e adattatori.

La sincronizzazione attiva di NetApp SnapMirror, disponibile su sistemi non MetroCluster e su sistemi ASA R2, offre una protezione granulare dei datastore con protocolli SAN FCP e iSCSI. Consente di proteggere l'intero vMSC o in modo selettivo i carichi di lavoro ad alta priorità. Offre l'accesso Active-Active ai siti locali e remoti, a differenza di NetApp MetroCluster, che è una soluzione Active-standby. A partire da ONTAP 9.15.1, SnapMirror Active Sync supporta una funzionalità Active/Active simmetrica, consentendo operazioni i/o in lettura e scrittura da entrambe le copie di un LUN protetto con replica sincrona bidirezionale, consentendo alle due copie LUN di servire le operazioni i/O. Prima di ONTAP 9.15.1, la sincronizzazione attiva di SnapMirror supporta solo configurazioni Active/Active asimmetriche, in cui i dati sul sito secondario sono sottoposti a proxy alla copia primaria di una LUN.

Per creare un cluster VMware ha/DRS su due siti, gli host ESXi vengono utilizzati e gestiti da un'appliance vCenter Server (VCSA). Le reti di gestione vSphere, vMotion® e delle macchine virtuali sono collegate tramite una rete ridondante tra i due siti. VCenter Server che gestisce il cluster ha/DRS può connettersi agli host ESXi in entrambi i siti e deve essere configurato utilizzando vCenter ha.

Fare riferimento a ["Come creare e configurare i cluster nel client vSphere"](#) Per configurare vCenter ha.

Fare riferimento anche a ["Procedure consigliate per VMware vSphere Metro Storage Cluster"](#).

Che cos'è vSphere Metro Storage Cluster?

vSphere Metro Storage Cluster (vMSC) è una configurazione certificata che protegge le macchine virtuali (VM) e i container dai guasti. Ciò si ottiene utilizzando concetti di storage esteso insieme a cluster di host ESXi, distribuiti su diversi domini di errore, come rack, edifici, campus o persino città. Le tecnologie di storage ActiveSync NetApp MetroCluster e SnapMirror vengono utilizzate per fornire una protezione con obiettivo di punto di ripristino zero (RPO=0) ai cluster host. La configurazione vMSC è progettata per garantire che i dati siano sempre disponibili anche in caso di guasto di un "sito" fisico o logico completo. Un dispositivo di archiviazione che fa parte della configurazione vMSC deve essere certificato dopo aver superato con successo il processo di certificazione vMSC. Tutti i dispositivi di archiviazione supportati possono essere trovati in ["Guida alla compatibilità dello storage VMware"](#).

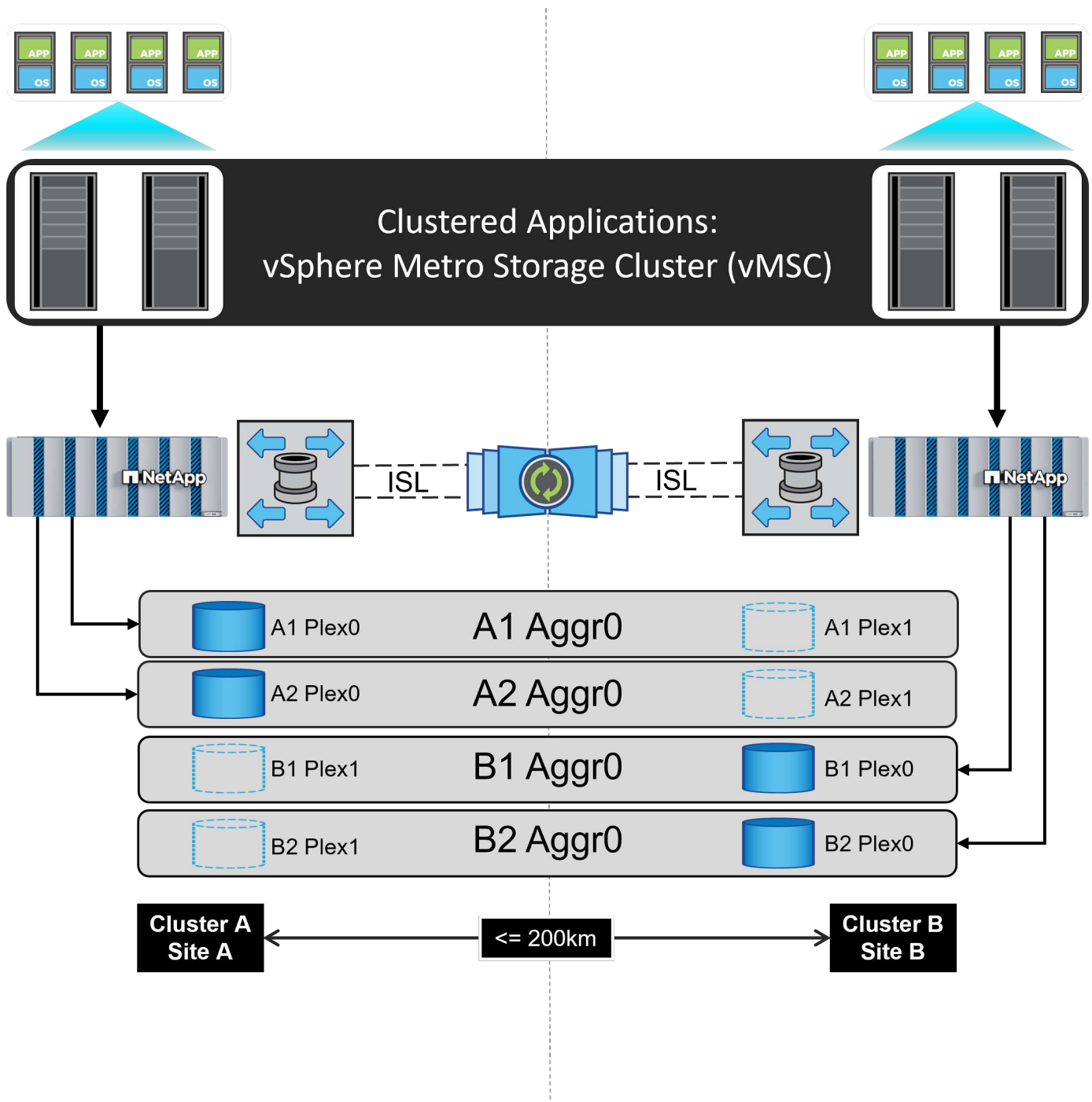
Per ulteriori informazioni sulle linee guida di progettazione per vSphere Metro Storage Cluster, consultare la seguente documentazione:

- ["Supporto di VMware vSphere con NetApp MetroCluster"](#)
- ["Supporto di VMware vSphere con business continuity di NetApp SnapMirror"](#) (Adesso noto come SnapMirror Active Sync)

NetApp MetroCluster può essere implementato in due configurazioni diverse per l'utilizzo con vSphere:

- Stretch MetroCluster
- Fabric MetroCluster

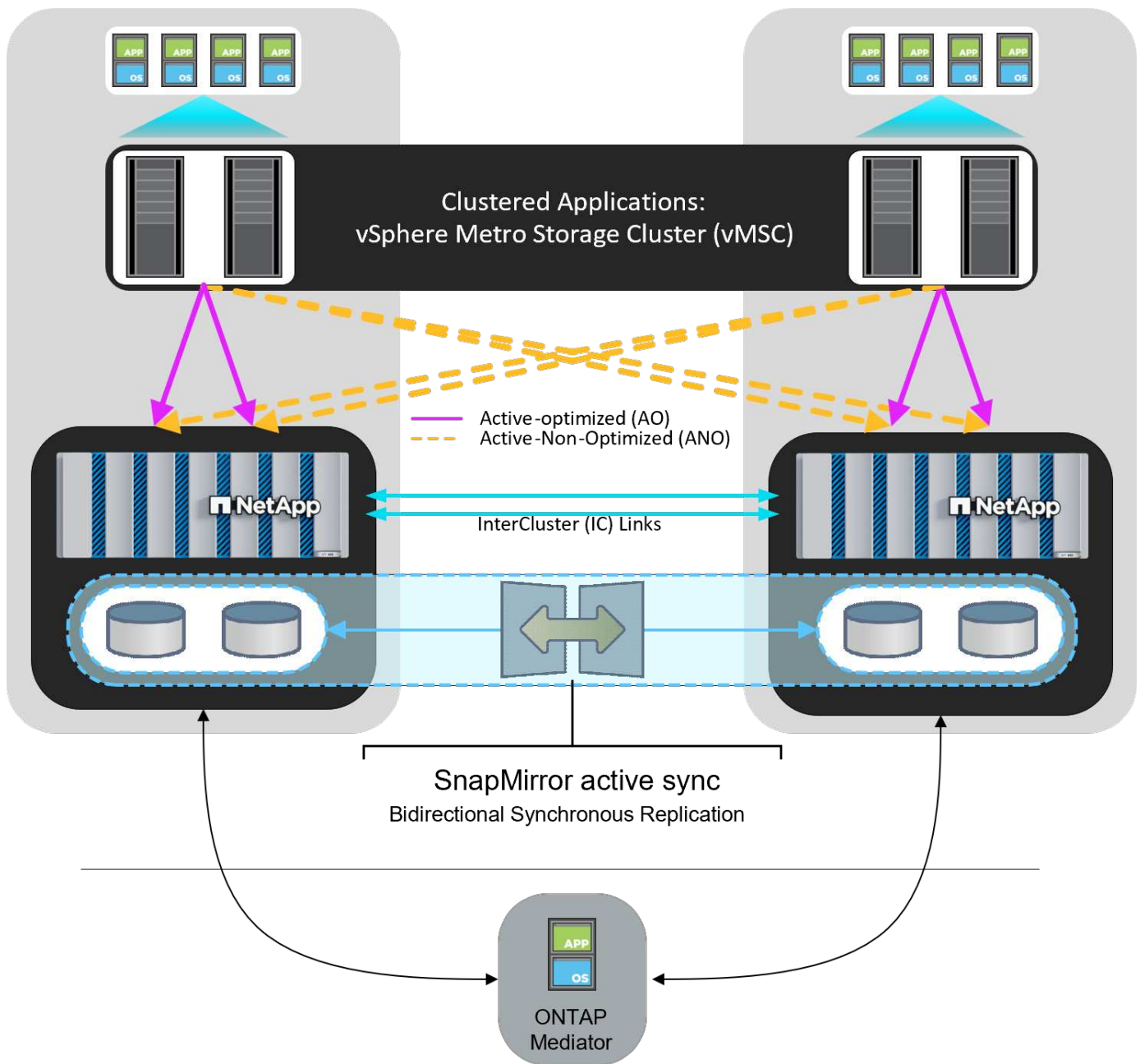
Di seguito viene illustrato uno schema topologico di alto livello di Stretch MetroCluster.



Fare riferimento a ["Documentazione MetroCluster"](#) Per informazioni specifiche sulla progettazione e la distribuzione di MetroCluster.

SnapMirror Active Sync può anche essere implementato in due modi diversi.

- Asimmetrico
- Active Sync simmetrico (ONTAP 9.15.1)



Per informazioni specifiche sulla progettazione e la distribuzione della sincronizzazione attiva di SnapMirror, consultare la sezione ["Documenti NetApp"](#).

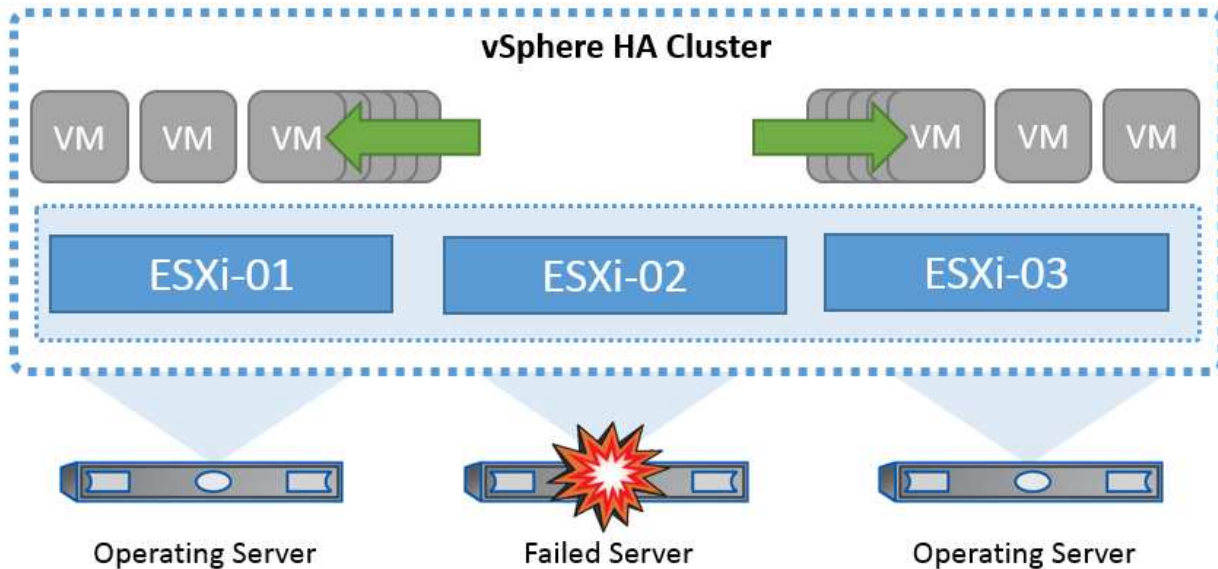
Panoramica della soluzione VMware vSphere

vCenter Server Appliance (VCSA) è un potente sistema di gestione centralizzata e un unico pannello di controllo per vSphere che consente agli amministratori di gestire in modo efficace i cluster ESXi. Facilita funzioni chiave quali il provisioning delle VM, il funzionamento di vMotion, l'alta disponibilità (HA), il Distributed Resource Scheduler (DRS), VMware vSphere Kubernetes Service (VKS) e molto altro. È un componente essenziale negli ambienti cloud VMware e dovrebbe essere progettato tenendo presente la disponibilità del servizio.

Alta disponibilità vSphere

La tecnologia cluster di VMware raggruppa i server ESXi in pool di risorse condivise per le macchine virtuali e fornisce vSphere High Availability (ha), offrendo un'elevata disponibilità e una semplicità d'uso per le applicazioni eseguite su macchine virtuali. Quando la funzionalità ha è abilitata sul cluster, ogni server ESXi mantiene la comunicazione con altri host in modo che, se un host ESXi non risponde o si isola, il cluster di ha può negoziare il recovery delle macchine virtuali in esecuzione sull'host ESXi tra gli host sopravvissuti nel cluster. In caso di errore del sistema operativo guest, vSphere ha può riavviare la macchina virtuale interessata sullo stesso server fisico. vSphere ha consente di ridurre i tempi di inattività pianificati, prevenire i tempi di inattività non pianificati e ripristinare rapidamente i dati in caso di interruzioni.

Cluster vSphere HA che ripristina le VM da un server guasto.



È importante comprendere che VMware vSphere non conosce la sincronizzazione attiva di NetApp MetroCluster o SnapMirror e vede tutti gli host ESXi nel cluster vSphere come host idonei per le operazioni del cluster ha in base alle configurazioni di affinità dei gruppi di host e VM.

Rilevamento errori host

Non appena viene creato il cluster HA, tutti gli host nel cluster partecipano all'elezione e uno degli host diventa master. Ogni slave esegue un heartbeat di rete verso il master, e il master, a sua volta, esegue un heartbeat di rete su tutti gli host slave. L'host master di un cluster vSphere HA è responsabile del rilevamento dei guasti degli host slave.

A seconda del tipo di errore rilevato, potrebbe essere necessario eseguire il failover delle macchine virtuali in esecuzione sugli host.

In un cluster vSphere ha, vengono rilevati tre tipi di errore dell'host:

- Errore - Un host smette di funzionare.
- Isolamento - Un host diventa isolato dalla rete.
- Partizione - Un host perde la connettività di rete con l'host master.

L'host master monitora gli host slave nel cluster. Questa comunicazione viene fatta attraverso lo scambio di heartbeat di rete ogni secondo. Quando l'host master smette di ricevere questi heartbeat da un host slave,

controlla la liveness dell'host prima di dichiarare che l'host non è riuscito. Il controllo liveness che l'ospite principale effettua è di determinare se l'ospite secondario sta scambiando i heartbeat con uno dei datastore. Inoltre, l'host master verifica se l'host risponde ai ping ICMP inviati ai propri indirizzi IP di gestione per rilevare se è semplicemente isolato dal suo nodo master o completamente isolato dalla rete. Per farlo, eseguire il ping del gateway predefinito. È possibile specificare manualmente uno o più indirizzi di isolamento per migliorare l'affidabilità della convalida dell'isolamento.



NetApp consiglia di specificare un minimo di due indirizzi di isolamento aggiuntivi e che ciascuno di questi indirizzi sia locale al sito. Ciò migliorerà l'affidabilità della convalida dell'isolamento.

Risposta di isolamento dell'host

Isolation Response è un'impostazione di vSphere HA che determina l'azione attivata sulle macchine virtuali quando un host in un cluster vSphere HA perde le sue connessioni di rete di gestione ma continua a funzionare. Sono disponibili tre opzioni per questa impostazione: "Disabilitato", "Arresta e riavvia le VM" e "Spegni e riavvia le VM".

"Arresta" è meglio di "Spegni", che non elimina le modifiche più recenti sul disco né esegue il commit delle transazioni. Se le macchine virtuali non si sono arrestate entro 300 secondi, vengono spente. Per modificare il tempo di attesa, utilizzare l'opzione avanzata `das.isolationshutdowntimeout`.

Prima che ha avvi la risposta di isolamento, verifica prima se l'agente master ha vSphere è proprietario del datastore che contiene i file di configurazione della VM. In caso contrario, l'host non attiverà la risposta di isolamento, poiché non vi è alcun master per riavviare le VM. L'host controllerà periodicamente lo stato del datastore per determinare se viene richiesto da un agente vSphere ha che detiene il ruolo master.



NetApp consiglia di impostare la risposta di isolamento dell'host su Disabilitato.

Una condizione split-brain può verificarsi se un host viene isolato o partizionato dall'host master vSphere ha e il master non è in grado di comunicare tramite datastore heartbeat o tramite ping. Il master dichiara l'host isolato inattivo e riavvia le macchine virtuali su altri host nel cluster. Esiste ora una condizione split-brain perché esistono due istanze della macchina virtuale in esecuzione, una sola delle quali è in grado di leggere o scrivere i dischi virtuali. Le condizioni split-brain possono ora essere evitate configurando VMCP (VM Component Protection).

Protezione dei componenti VM (VMCP)

Uno dei miglioramenti delle funzionalità di vSphere 6, relativi all'ha, è VMCP. VMCP fornisce una protezione avanzata da APD (All Path Down) e PDL (Permanent Device Loss) per lo storage a blocchi (FC, iSCSI, FCoE) e a file (NFS).

Perdita permanente del dispositivo (PDL)

PDL è una condizione che si verifica quando un dispositivo di archiviazione si guasta in modo permanente o viene rimosso amministrativamente e non si prevede che verrà ripristinato. L'array di archiviazione NetApp invia un codice SCSI Sense a ESXi, dichiarando che il dispositivo è stato perso definitivamente. Nella sezione Condizioni di errore e risposta della VM di vSphere HA, è possibile configurare la risposta da adottare dopo il rilevamento di una condizione PDL.



NetApp consiglia di impostare la "Risposta per Datastore con PDL" su **"Spegni e riavvia le VM"**. Quando viene rilevata questa condizione, una VM verrà riavviata immediatamente su un host funzionante all'interno del cluster vSphere HA.

Tutti i percorsi verso il basso (APD)

APD è una condizione che si verifica quando un dispositivo di archiviazione diventa inaccessibile all'host e non sono disponibili percorsi verso l'array. ESXi ritiene che si tratti di un problema temporaneo del dispositivo e si aspetta che torni disponibile.

Quando viene rilevata una condizione APD, viene avviato un timer. Dopo 140 secondi, la condizione APD viene dichiarata ufficialmente e il dispositivo viene contrassegnato come timeout APD. Una volta trascorsi i 140 secondi, ha inizia il conteggio dei minuti specificati nell'APD Delay for VM failover. Una volta trascorso il tempo specificato, ha riavvia le macchine virtuali interessate. È possibile configurare VMCP in modo che risponda in modo diverso, se lo si desidera (Disattivato, Eventi problema o Spegni e riavvia le macchine virtuali).



- NetApp consiglia di configurare "Risposta per datastore con APD" su **"Spegni e riavvia le VM (conservative)"**.
- Con "conservativo" si intende la probabilità che HA sia in grado di riavviare le VM. Se impostato su Conservativo, HA riavvierà la VM interessata dall'APD solo se sa che un altro host può riavviarla. Nel caso di Aggressive, HA tenterà di riavviare la VM anche se non conosce lo stato degli altri host. Ciò può comportare il mancato riavvio delle VM se non è presente alcun host con accesso al datastore in cui si trovano.
- Se lo stato APD viene risolto e l'accesso allo storage viene ripristinato prima che sia trascorso il timeout, ha non riavvierà inutilmente la macchina virtuale a meno che non sia stata esplicitamente configurata. Se si desidera una risposta anche quando l'ambiente è stato ripristinato dalla condizione APD, è necessario configurare la risposta per il ripristino APD dopo il timeout APD in modo da ripristinare le VM.
- NetApp consiglia di configurare la risposta per il ripristino APD dopo il timeout APD su Disabilitato.

Implementazione di VMware DRS per NetApp SnapMirror Active Sync

VMware DRS è una funzionalità che aggrega le risorse host in un cluster e viene utilizzata principalmente per il bilanciamento del carico all'interno di un cluster in un'infrastruttura virtuale. VMware DRS calcola principalmente le risorse di CPU e memoria per eseguire il bilanciamento del carico in un cluster. Poiché vSphere non è consapevole del clustering allungato, considera tutti gli host in entrambi i siti durante il bilanciamento del carico.

Implementazione VMware DRS per NetApp MetroCluster

To avoid cross-site traffic, NetApp recommends configuring DRS affinity rules to manage a logical separation of VMs. This will ensure that, unless there is a complete site failure, HA and DRS will only use local hosts. Se si crea una regola di affinità DRS per il cluster, è possibile specificare in che modo vSphere applica tale regola durante il failover di una macchina virtuale.

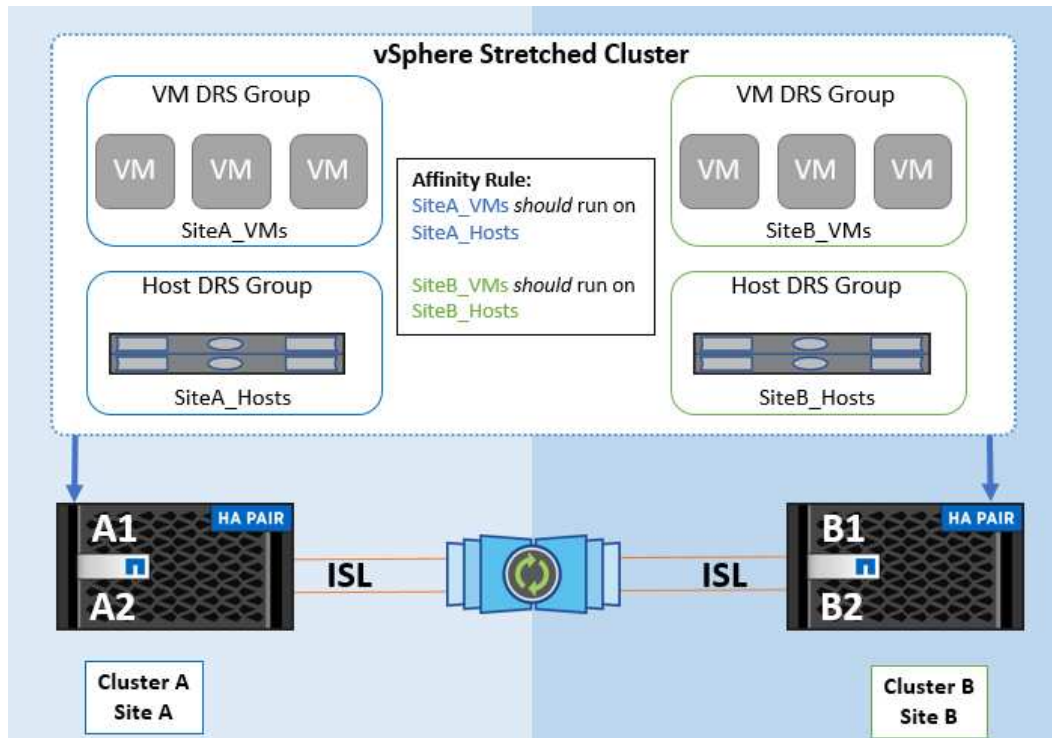
Esistono due tipi di regole che è possibile specificare per il comportamento del failover di vSphere HA:

- Le regole di anti-affinità delle macchine virtuali costringono le macchine virtuali specificate a rimanere separate durante le azioni di failover.
- Le regole di affinità degli host VM collocano macchine virtuali specifiche su un host specifico o su un

membro di un gruppo definito di host durante le azioni di failover.

Utilizzando le regole di affinità degli host delle macchine virtuali in VMware DRS, si può avere una separazione logica tra il sito A e il sito B in modo che la macchina virtuale venga eseguita sull'host nello stesso sito dell'array configurato come controller di lettura/scrittura principale per un determinato datastore. Inoltre, le regole di affinità degli host delle macchine virtuali consentono alle macchine virtuali di rimanere locali rispetto allo storage, il che a sua volta determina la connessione della macchina virtuale in caso di errori di rete tra i siti.

Di seguito è riportato un esempio di gruppi di host VM e regole di affinità.



Best practice

NetApp consiglia di implementare regole "should" invece di regole "must", in quanto vengono violate da vSphere ha in caso di errore. L'utilizzo di regole "must" potrebbe potenzialmente causare interruzioni del servizio.

La disponibilità dei servizi dovrebbe sempre prevalere sulle prestazioni. Nello scenario in cui un data center completo fallisce, le regole "must" devono scegliere gli host dal gruppo di affinità degli host delle VM e, quando il data center non è disponibile, le macchine virtuali non verranno riavviate.

Implementazione di VMware Storage DRS con NetApp MetroCluster

La funzionalità VMware Storage DRS consente l'aggregazione di datastore in una singola unità e bilancia i dischi della macchina virtuale quando vengono superate le soglie di controllo i/o di storage (SIOC).

Il controllo i/o dello storage è abilitato per impostazione predefinita sui cluster DRS abilitati per Storage DRS. Il controllo i/o dello storage consente a un amministratore di controllare la quantità di i/o dello storage allocata alle macchine virtuali nei periodi di congestione dell'i/o e di conseguenza le macchine virtuali più importanti possono preferire le macchine virtuali meno importanti per l'allocazione delle risorse i/o.

Storage DRS utilizza Storage vMotion per migrare le macchine virtuali in datastore diversi all'interno di un

cluster di datastore. In un ambiente NetApp MetroCluster, la migrazione di una macchina virtuale deve essere controllata all'interno dei datastore di quel sito. Ad esempio, la macchina virtuale A, in esecuzione su un host nel sito A, dovrebbe idealmente migrare all'interno dei datastore della SVM nel sito A. In caso contrario, la macchina virtuale continuerà a funzionare ma con prestazioni ridotte, poiché la lettura/scrittura del disco virtuale avverrà dal sito B attraverso collegamenti tra siti.

*Quando si utilizza l'archiviazione ONTAP, si consiglia di disattivare l'archiviazione DRS.



- I DRS di archiviazione non sono generalmente necessari o consigliati per l'uso con i sistemi di archiviazione ONTAP.
- ONTAP offre proprie funzionalità di efficienza dello storage, come deduplica, compressione e compaction, che possono essere influenzate dallo Storage DRS.
- Se si utilizzano snapshot ONTAP, Storage vMotion lascerebbe indietro la copia della VM nello snapshot, aumentando potenzialmente l'utilizzo dello storage e potrebbe avere un impatto sulle applicazioni di backup come NetApp SnapCenter, che tiene traccia delle VM e dei relativi snapshot ONTAP.

Linee guida per la progettazione e l'implementazione di vMSC

Questo documento delinea le linee guida di progettazione e implementazione per vMSC con i sistemi di storage ONTAP.

Configurazione dello storage NetApp

Le istruzioni per l'installazione di NetApp MetroCluster sono disponibili all'indirizzo ["Documentazione MetroCluster"](#). Le istruzioni per SnapMirror Active Sync (SMA) sono disponibili anche all'indirizzo ["Panoramica di SnapMirror Business Continuity"](#).

Una volta configurato MetroCluster, gestirlo è come gestire un ambiente ONTAP tradizionale. Puoi configurare Storage Virtual Machine (SVM) utilizzando vari strumenti come l'interfaccia a riga di comando (CLI), System Manager o Ansible. Una volta configurate le SVM, occorre creare nel cluster interfacce logiche (LIF), volumi e LUN (Logical Unit Number) da utilizzare per le normali operazioni. Questi oggetti verranno replicati automaticamente sull'altro cluster utilizzando la rete di peering del cluster.

Se non utilizzi MetroCluster, o se disponi di sistemi ONTAP non supportati per MetroCluster, come ad esempio i sistemi ASA R2, puoi utilizzare SnapMirror Active Sync che fornisce una protezione granulare dei datastore e l'accesso Active-Active su più cluster ONTAP in diversi domini di errore. SMA utilizza gruppi di coerenza (CGS) per garantire la coerenza dell'ordine di scrittura tra uno o più datastore ed è possibile creare più CGS in base ai requisiti dell'applicazione e del datastore. I gruppi di coerenza sono particolarmente utili per le applicazioni che richiedono la sincronizzazione dei dati tra datastore multipli. Ad esempio, LVM guest distribuiti tra datastore. SMA supporta inoltre RDM (Raw Device Mapping) e storage connesso al guest con iniziatori iSCSI in-guest. Per ulteriori informazioni sui gruppi di coerenza, visitare il sito Web all'indirizzo ["Panoramica dei gruppi di coerenza"](#).

Esiste una certa differenza nella gestione di una configurazione vMSC con sincronizzazione attiva SnapMirror rispetto a una MetroCluster. In primo luogo, SMA è una configurazione solo SAN, nessun datastore NFS può essere protetto con la sincronizzazione attiva di SnapMirror. In secondo luogo, è necessario mappare entrambe le copie delle LUN agli host ESXi per accedere ai datastore replicati in entrambi i domini di errore. Terzo, devi creare uno o più gruppi di coerenza per i datastore da proteggere con la sincronizzazione attiva di SnapMirror. Infine, è necessario creare un criterio SnapMirror per i gruppi di coerenza creati. Tutto questo può

essere fatto facilmente usando la procedura guidata "Protect cluster" nel plug-in vCenter di ONTAP tools, o usando manualmente la CLI di ONTAP o System Manager.

Utilizzo del plug-in vCenter di ONTAP Tools per SnapMirror Active Sync

Il plug-in vCenter degli strumenti ONTAP fornisce un modo semplice e intuitivo per configurare SnapMirror Active Sync per vMSC. Puoi usare il plug-in vCenter di ONTAP Tools per creare e gestire relazioni di sincronizzazione attive di SnapMirror tra due cluster ONTAP. Questo plugin fornisce un'interfaccia di facile utilizzo per stabilire e gestire queste relazioni in modo efficiente. Per ulteriori informazioni sul plug-in vCenter degli strumenti ONTAP, visitare il sito Web all'indirizzo "[Strumenti ONTAP per VMware vSphere](#)", oppure accedere direttamente a "[Proteggere utilizzando la protezione del cluster host](#)".

Configurazione di VMware vSphere

Creare un cluster vSphere ha

La creazione di un cluster vSphere ha è un processo in più fasi documentato all'indirizzo "[Come creare e configurare i cluster nel client vSphere su docs.vmware.com](#)". In poche parole, devi prima creare un cluster vuoto, quindi, utilizzando vCenter, devi aggiungere host e specificare l'ha vSphere del cluster e le altre impostazioni.



Nessuna disposizione del presente documento sostituisce "[Procedure consigliate per VMware vSphere Metro Storage Cluster](#)". Questo contenuto viene fornito a scopo di riferimento e non sostituisce la documentazione ufficiale VMware.

Per configurare un cluster ha, completare i seguenti passaggi:

1. Connettersi all'interfaccia utente di vCenter.
2. In host e cluster, individuare il data center in cui si desidera creare il cluster ha.
3. Fare clic con il pulsante destro del mouse sull'oggetto del data center e selezionare nuovo cluster. In base alle nozioni di base, assicurarsi di aver abilitato vSphere DRS e vSphere ha. Completare la procedura guidata.

New Cluster

1 Basics

2 Image

3 Review

Basics

Name MCC Cluster

Location Raleigh

vSphere DRS ☒

vSphere HA ☒

vSAN ☐ Enable vSAN ESA

☒ Manage all hosts in the cluster with a single image

Choose how to set up the cluster's image

☒ Compose a new image

☐ Import image from an existing host in the vCenter inventory

☐ Import image from a new host

☐ Manage configuration at a cluster level

1. Selezionare il cluster e accedere alla scheda di configurazione. Selezionare vSphere ha e fare clic su

Modifica.

2. In monitoraggio host, selezionare l'opzione attiva monitoraggio host.

Edit Cluster Settings | MCC Cluster

vSphere HA ☒

Failures and responses | Admission Control | Heartbeat Datastores | Advanced Options

You can configure how vSphere HA responds to the failure conditions on this cluster. The following failure conditions are supported: host, host isolation, VM component protection (datastore with PDL and APD), VM and application.

Enable Host Monitoring ⓘ ☒

> Host Failure Response	Restart VMs ▾
> Response for Host Isolation	Disabled ▾
> Datastore with PDL	Power off and restart VMs ▾
> Datastore with APD	Power off and restart VMs - Conservative restart policy ▾
> VM Monitoring	Disabled ▾

CANCEL

OK

1. Nella scheda guasti e risposte, in monitoraggio VM, selezionare l'opzione solo monitoraggio VM o monitoraggio VM e applicazione.

> Response for Host Isolation Disabled

> Datastore with PDL Power off and restart VMs

> Datastore with APD Power off and restart VMs - Conservative restart policy

▼ VM Monitoring

Enable heartbeat monitoring

VM monitoring resets individual VMs if their VMware tools heartbeats are not received within a set time. Application monitoring resets individual VMs if their in-guest heartbeats are not received within a set time.

☐ Disabled

☐ VM Monitoring Only

Turns on VMware tools heartbeats. When heartbeats are not received within a set time, the VM is reset.

☒ VM and Application Monitoring

Turns on application heartbeats. When heartbeats are not received within a set time, the VM is reset.

CANCEL OK

1. In controllo ammissione, impostare l'opzione di controllo ammissione ha su Cluster Resource Reserve; utilizzare 50% CPU/MEM.

Edit Cluster Settings | MCC Cluster



vSphere HA ☒

Failures and responses Admission Control Heartbeat Datastores Advanced Options

Admission control is a policy used by vSphere HA to ensure failover capacity within a cluster. Raising the number of potential host failures will increase the availability constraints and capacity reserved.

Host failures cluster tolerates

1

Maximum is one less than number of hosts in cluster.

Define host failover capacity by

Cluster resource Percentage

☒ Override calculated failover capacity.

Reserved failover CPU capacity: 50 % CPU

Reserved failover Memory capacity: 50 % Memory

☐ Reserve Persistent Memory failover capacity

☐ Override calculated Persistent Memory failover capacity

CANCEL

OK

1. Fare clic su "OK".
2. Selezionare DRS e fare clic su MODIFICA.
3. Impostare il livello di automazione su manuale, a meno che non sia richiesto dalle applicazioni.

Edit Cluster Settings | MCC Cluster



vSphere DRS ☒

Automation Additional Options Power Management Advanced Options

Automation Level

Manual

DRS generates both power-on placement recommendations, and migration recommendations for virtual machines. Recommendations need to be manually applied or ignored.

Migration Threshold

Conservative
(Less
Frequent
vMotions)

(3) DRS provides recommendations when workloads are moderately imbalanced. This threshold is suggested for environments with stable workloads. (Default)

Aggressive
(More
Frequent
vMotions)

Predictive DRS

☐ Enable

Virtual Machine Automation

☒ Enable

1. Abilitare la protezione dei componenti VM, fare riferimento a. ["docs.vmware.com"](https://docs.vmware.com).
2. Le seguenti impostazioni aggiuntive di vSphere ha sono consigliate per vMSC con MetroCluster:

Guasto	Risposta
Errore host	Riavviare le VM
Isolamento degli host	Disattivato
Datastore con perdita permanente di dispositivi (PDL)	Spegnere e riavviare le macchine virtuali
Datastore con tutti i percorsi verso il basso (APD)	Spegnere e riavviare le macchine virtuali
L'ospite non batte il cuore	Ripristinare le VM
Policy di riavvio della VM	Determinato dall'importanza della VM
Risposta per l'isolamento dell'host	Arrestare e riavviare le VM
Risposta per il datastore con PDL	Spegnere e riavviare le macchine virtuali
Risposta per datastore con APD	Spegnere e riavviare le macchine virtuali (conservative)
Ritardo del failover delle macchine virtuali per APD	3 minuti
Risposta per il ripristino APD con timeout APD	Disattivato
Sensibilità di monitoraggio VM	Preimpostazione alta

Configurare gli archivi dati per Heartbeating

VSphere ha utilizza i datastore per monitorare gli host e le macchine virtuali in caso di guasto alla rete di gestione. È possibile configurare in che modo vCenter seleziona i datastore heartbeat. Per configurare gli archivi dati per il heartbeat, completare i seguenti passaggi:

1. Nella sezione Heartbeating del datastore, selezionare Usa archivi dati dall'elenco specificato e completare automaticamente se necessario.
2. Seleziona i datastore che desideri utilizzare vCenter da entrambi i siti e premi OK.

vSphere HA 

Failures and responses

Admission Control

Heartbeat Datastores









Advanced Options

vSphere HA uses datastores to monitor hosts and virtual machines when the HA network has failed. vCenter Server selects 4 datastores for each host using the policy and datastore preferences specified below.

Heartbeat datastore selection policy:

- ☐ Automatically select datastores accessible from the hosts
- ☐ Use datastores only from the specified list
- ☒ Use datastores from the specified list and complement automatically if needed

Available heartbeat datastores

	Name ↑	Datastore Cluster	Hosts Mounting Datastore
<input checked="" type="checkbox"/>	 d11	N/A	2
<input checked="" type="checkbox"/>	 d12	N/A	2
<input checked="" type="checkbox"/>	 d21	N/A	2
<input checked="" type="checkbox"/>	 d22	N/A	2
<input type="checkbox"/>	 d31	N/A	2
<input type="checkbox"/>	 d32	N/A	2
<input type="checkbox"/>	 d41	N/A	2
<input type="checkbox"/>	 d42	N/A	2

11 items

CANCEL

OK

Configurare le opzioni avanzate

Gli eventi di isolamento si verificano quando gli host all'interno di un cluster ha perduto la connettività alla rete o ad altri host nel cluster. Per impostazione predefinita, vSphere ha utilizzato il gateway predefinito per la propria rete di gestione come indirizzo di isolamento predefinito. Tuttavia, è possibile specificare indirizzi di isolamento aggiuntivi per l'host al ping per determinare se deve essere attivata una risposta di isolamento. Aggiungere due IP di isolamento in grado di eseguire il ping, uno per sito. Non utilizzare l'indirizzo IP del gateway. L'impostazione avanzata vSphere ha utilizzato è `das.isolationaddress`. A tale scopo, è possibile utilizzare gli indirizzi IP ONTAP o Mediator.

Fare riferimento a ["Procedure consigliate per VMware vSphere Metro Storage Cluster"](#) per ulteriori informazioni.

vSphere HA ☒

Failures and responses

Admission Control

Heartbeat Datastores

Advanced Options

You can set advanced options that affect the behavior of your vSphere HA cluster.

[+ Add](#) [✕ Delete](#)

Option	Value
das.ignoreRedundantNetWarning	true
das.isolationaddress0	10.61.99.100
das.isolationaddress1	10.61.99.110
das.heartbeatDsPerHost	4
4 items	

CANCEL

OK

L'aggiunta di un'impostazione avanzata denominata `das.heartbeatDsPerHost` può aumentare il numero di datastore heartbeat. Utilizzare quattro datastore heartbeat (HB DSS), due per sito. Utilizzare l'opzione "Seleziona dall'elenco ma complimento". Questo è necessario perché se un sito non funziona, è necessario ancora due HB DSS. Tuttavia, questi elementi non devono essere protetti con la sincronizzazione attiva di MetroCluster o SnapMirror.

Fare riferimento a ["Procedure consigliate per VMware vSphere Metro Storage Cluster"](#) per ulteriori informazioni.

Affinità con VMware DRS per NetApp MetroCluster

In questa sezione vengono creati gruppi DRS per VM e host per ciascun sito/cluster nell'ambiente MetroCluster. Quindi configuriamo le regole VM/host per allineare l'affinità dell'host VM con le risorse di storage locali. Ad esempio, il sito A fa parte del gruppo VM `sitea_vm` e gli host del sito A appartengono al gruppo host `sitea_hosts`. Successivamente, in VM/host Rules, si afferma che `sitea_vm` deve essere eseguito sugli host in `sitea_hosts`.



- NetApp consiglia vivamente la specifica **deve essere eseguita sugli host nel gruppo** piuttosto che sulla specifica **deve essere eseguita sugli host nel gruppo**. In caso di guasto dell'host del sito A, è necessario riavviare le macchine virtuali del sito A sugli host del sito B attraverso vSphere ha, ma quest'ultima specifica non consente all'ha di riavviare le macchine virtuali sul sito B perché è una regola rigida. La specifica precedente è una regola debole e viene violata in caso di ha, abilitando in tal modo la disponibilità anziché le prestazioni.
- È possibile creare un allarme basato su eventi che viene attivato quando una macchina virtuale viola una regola di affinità VM-host. Nel client vSphere, aggiungere un nuovo allarme per la macchina virtuale e selezionare "VM is Violating VM-host Affinity Rule" (VM viola la regola di affinità VM-host) come trigger dell'evento. Per ulteriori informazioni sulla creazione e la modifica degli allarmi, consultare "[Monitoraggio e performance di vSphere](#)" la documentazione.

Creare gruppi host DRS

Per creare gruppi di host DRS specifici per il sito A e il sito B, attenersi alla seguente procedura:

1. Nel client web vSphere, fare clic con il pulsante destro del mouse sul cluster nell'inventario e selezionare Impostazioni.
2. Fare clic su VM\host Groups.
3. Fare clic su Aggiungi.
4. Digitare il nome del gruppo (ad esempio, sitea_hosts).
5. Dal menu tipo, selezionare Gruppo host.
6. Fare clic su Aggiungi e selezionare gli host desiderati dal sito A, quindi fare clic su OK.
7. Ripetere questi passaggi per aggiungere un altro gruppo di host per il sito B.
8. Fare clic su OK.

Creare gruppi DRS VM

Per creare gruppi di macchine virtuali DRS specifici per il sito A e il sito B, attenersi alla seguente procedura:

1. Nel client web vSphere, fare clic con il pulsante destro del mouse sul cluster nell'inventario e selezionare Impostazioni.
2. Fare clic su VM\host Groups.
3. Fare clic su Aggiungi.
4. Digitare il nome del gruppo (ad esempio, sitea_vm).
5. Dal menu tipo, selezionare Gruppo VM.
6. Fare clic su Add (Aggiungi) e selezionare le VM desiderate dal sito A, quindi fare clic su OK.
7. Ripetere questi passaggi per aggiungere un altro gruppo di host per il sito B.
8. Fare clic su OK.

Crea regole host VM

Per creare regole di affinità DRS specifiche per il sito A e il sito B, completare i seguenti passaggi:

1. Nel client web vSphere, fare clic con il pulsante destro del mouse sul cluster nell'inventario e selezionare

Impostazioni.

2. Fare clic su VM\host Rules.
3. Fare clic su Aggiungi.
4. Digitare il nome della regola (ad esempio, sitea_Affinity).
5. Verificare che l'opzione Enable Rule (attiva regola) sia selezionata.
6. Dal menu Type (tipo), selezionare Virtual Machines to hosts (macchine virtuali a host).
7. Selezionare il gruppo VM (ad esempio, sitea_vm).
8. Selezionare il gruppo host (ad esempio, sitea_hosts).
9. Ripetere questi passaggi per aggiungere un'altra VM\regola host per il sito B.
10. Fare clic su OK.

Create VM/Host Rule | Cluster-01 ×

Name	sitea_affinity	<input checked="" type="checkbox"/> Enable rule.
Type	Virtual Machines to Hosts ▼	

Virtual machines that are members of the Cluster VM Group sitea_vms should run on host group sitea_hosts.

VM Group:

sitea_vms	▼
Should run on hosts in group	▼

Host Group:

sitea_hosts	▼
-------------	---

CANCEL OK

Crea cluster di datastore se necessario

Per configurare un cluster di datastore per ciascun sito, attenersi alla seguente procedura:

1. Utilizzando il client web vSphere, individuare il data center in cui risiede il cluster ha in Storage.
2. Fare clic con il pulsante destro del mouse sull'oggetto del data center e selezionare Storage > New Datastore Cluster.

*Quando si utilizza l'archiviazione ONTAP, si consiglia di disattivare l'archiviazione DRS.



- I DRS di archiviazione non sono generalmente necessari o consigliati per l'uso con i sistemi di archiviazione ONTAP.
- ONTAP offre proprie funzionalità di efficienza dello storage, come deduplica, compressione e compaction, che possono essere influenzate dallo Storage DRS.
- Se si utilizzano snapshot ONTAP, storage vMotion lascerebbe la copia della macchina virtuale nella snapshot, aumentando potenzialmente l'utilizzo dello storage e potrebbe avere un impatto sulle applicazioni di backup, come NetApp SnapCenter, che tengono traccia delle macchine virtuali e delle relative snapshot ONTAP.

Storage DRS automation

Cluster automation level

☒ **No Automation (Manual Mode)**
vCenter Server will make migration recommendations for virtual machine storage, but will not perform automatic migrations.

☐ **Fully Automated**
Files will be migrated automatically to optimize resource usage.

1. Selezionare il cluster ha e fare clic su Next.

New Datastore Cluster

1 Name and Location
2 Storage DRS Automation
3 Storage DRS Runtime Settings
4 **Select Clusters and Hosts**
5 Select Datastores
6 Ready to Complete

Select all hosts and clusters that require connectivity to the datastores in the datastore cluster.

Filter (1) Selected Objects

Clusters Standalone Hosts

Filter

Name
<input checked="" type="checkbox"/> MCC HA Cluster

1. Selezionare gli archivi dati appartenenti al sito A e fare clic su Avanti.

New Datastore Cluster

1 Name and Location
2 **Storage DRS Automation**
3 Storage DRS Runtime Settings
4 Select Clusters and Hosts
5 **Select Datastores**
6 Ready to Complete

Show datastores connected to all hosts

Filter

Name	Host Connection Status	Capacity	Free Space	Type
<input checked="" type="checkbox"/> sitea_infra	All Hosts Connect...	10.00 GB	10.00 GB	NFS
<input checked="" type="checkbox"/> sitea_infra2	All Hosts Connect...	10.00 GB	10.00 GB	NFS

1. Rivedere le opzioni e fare clic su fine.

2. Ripetere questa procedura per creare il cluster di datastore del sito B e verificare che siano selezionati solo i datastore del sito B.

Disponibilità di vCenter Server

Le appliance vCenter Server (VCSA) devono essere protette con vCenter ha. VCenter ha ti consente di implementare due VCSA in una coppia ha Active-passive. Uno in ogni dominio di errore. Puoi leggere ulteriori informazioni su vCenter ha all'indirizzo ["docs.vmware.com"](https://docs.vmware.com).

Resilienza per eventi pianificati e non pianificati

NetApp MetroCluster e SnapMirror Active Sync sono potenti strumenti che migliorano l'alta disponibilità e le operazioni senza interruzioni dell'hardware NetApp e del software ONTAP®.

Questi strumenti garantiscono una protezione a livello di sito per l'intero ambiente di storage, garantendo che i tuoi dati siano sempre disponibili. Che si stia utilizzando server standalone, cluster di server ad alta disponibilità, container o server virtualizzati, la tecnologia NetApp permette di conservare perfettamente la disponibilità dello storage in caso di black-out totale causato da black-out, raffreddamento o connettività di rete, arresto dello storage array o errori operativi.

La sincronizzazione attiva di MetroCluster e SnapMirror offre tre metodi di base per la continuità dei dati in caso di eventi pianificati o non pianificati:

- Componenti ridondanti per la protezione contro i guasti a un singolo componente
- Takeover locale di ha in caso di eventi che colpiscono un singolo controller
- Protezione completa del sito: Rapida ripresa del servizio mediante il trasferimento dello storage e dell'accesso client dal cluster di origine al cluster di destinazione

Ciò significa che le operazioni continuano senza problemi in caso di guasto a un singolo componente e vengono ripristinate automaticamente al funzionamento ridondante una volta sostituito il componente guasto.

Tutti i cluster ONTAP, ad eccezione dei cluster a nodo singolo (in genere versioni software-defined, come ad esempio ONTAP Select), offrono funzionalità di ha integrate chiamate takeover e giveback. Ciascun controller del cluster è accoppiato con un altro controller in modo da formare una coppia ha. Queste coppie garantiscono che ogni nodo sia connesso localmente allo storage.

Il takeover è un processo automatizzato in cui un nodo assume il controllo dello storage dell'altro per la gestione dei servizi dati. Giveback è il processo inverso che ripristina il normale funzionamento. Il takeover può essere pianificato, ad esempio durante la manutenzione hardware o gli upgrade della ONTAP, o non pianificato, derivante da un nodo di panico o da un guasto dell'hardware.

Durante un takeover, le LIF NAS nelle configurazioni MetroCluster eseguono automaticamente il failover. Tuttavia, le LIF SAN non vengono sottoposte a failover e continueranno a utilizzare il percorso diretto dei LUN (Logical Unit Number).

Per ulteriori informazioni sul takeover e sullo sconto ha, consultare la ["Panoramica sulla gestione delle coppie HA"](#). È importante notare che questa funzionalità non è specifica per MetroCluster o SnapMirror Active Sync.

Lo switchover del sito con MetroCluster viene eseguito quando un sito è offline o come attività pianificata per la manutenzione di un intero sito. Il sito rimanente presuppone la proprietà delle risorse storage (dischi e aggregati) del cluster offline e le SVM del sito guasto vengono messe online e riavviate nel sito di disaster recovery, preservando la loro identità completa per l'accesso client e host.

Con la sincronizzazione attiva di SnapMirror, poiché entrambe le copie vengono utilizzate contemporaneamente in modo attivo, gli host esistenti continueranno a funzionare. Il ONTAP Mediator è necessario per garantire che il failover del sito avvenga correttamente.

Scenari di errore per vMSC con MetroCluster

Nelle sezioni seguenti vengono illustrati i risultati attesi da vari scenari di guasto con i

sistemi vMSC e NetApp MetroCluster.

Errore singolo percorso di storage

In questo scenario, se componenti come la porta HBA, la porta di rete, la porta dello switch dati front-end o un cavo FC o Ethernet si guastano, quel particolare percorso al dispositivo di storage viene contrassegnato come inattivo dall'host ESXi. Se vengono configurati diversi percorsi per il dispositivo storage fornendo resilienza alla porta HBA/rete/switch, ESXi esegue uno switchover del percorso. Durante questo periodo, le macchine virtuali rimangono in esecuzione senza alcun impatto, perché la disponibilità dello storage viene garantita attraverso l'offerta di più percorsi al dispositivo di storage.



In questo scenario non vi sono cambiamenti nel comportamento di MetroCluster e tutti i datastore continuano a essere intatti dai rispettivi siti.

Best practice

Negli ambienti in cui vengono utilizzati volumi NFS/iSCSI, NetApp consiglia di avere almeno due uplink di rete configurati per la porta vmkernel NFS nel vSwitch standard e lo stesso nel gruppo di porte in cui è mappata l'interfaccia vmkernel NFS per il vSwitch distribuito. Il raggruppamento NIC può essere configurato in modalità Active-Active o Active-standby.

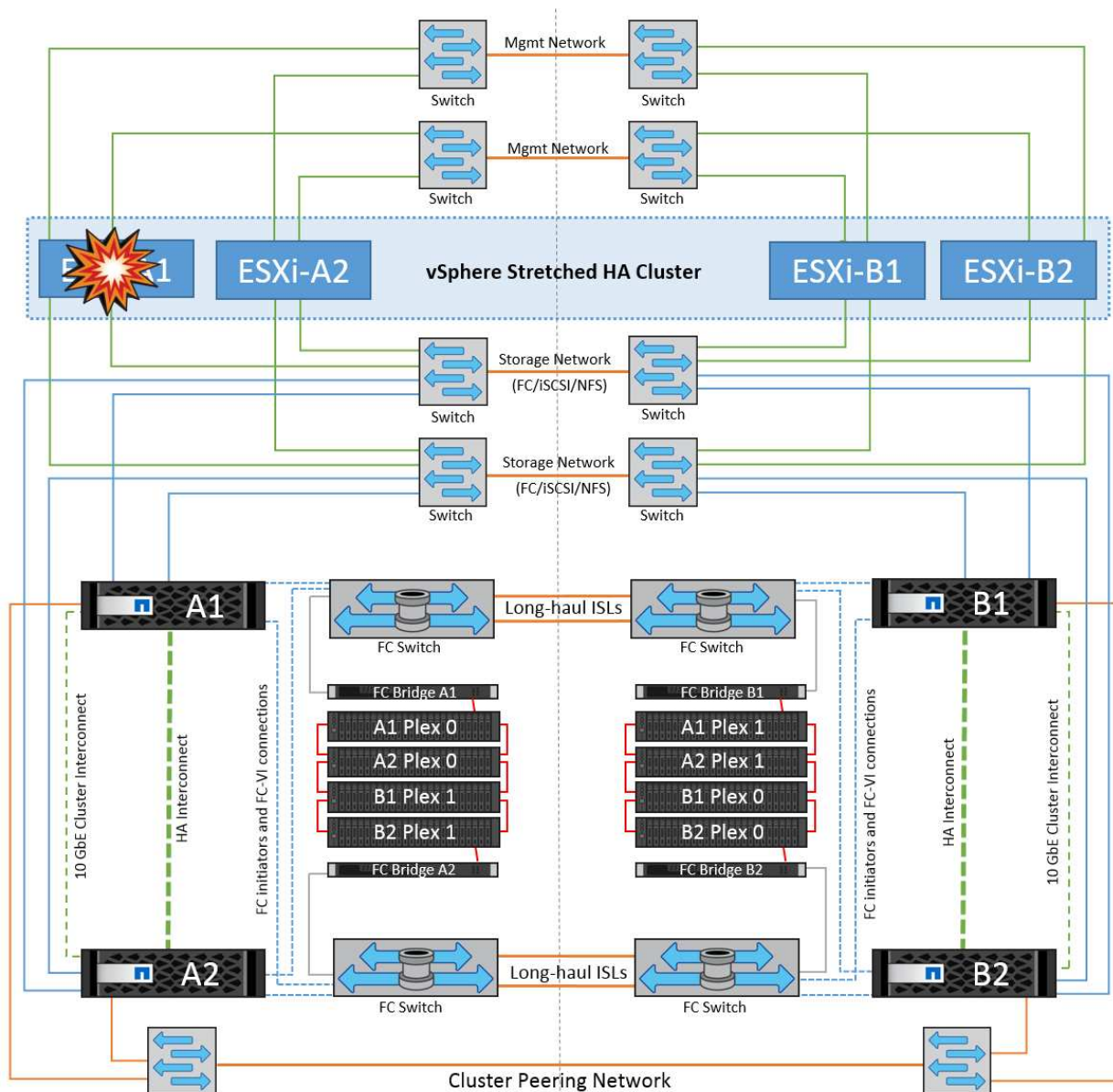
Inoltre, per i LUN iSCSI, il multipathing deve essere configurato legando le interfacce vmkernel agli adattatori di rete iSCSI. Per ulteriori informazioni, fai riferimento alla documentazione dello storage vSphere.

Best practice

Negli ambienti in cui vengono utilizzate le LUN Fibre Channel, NetApp consiglia di disporre di almeno due HBA, che garantiscono resilienza a livello di HBA/porta. NetApp consiglia inoltre di utilizzare lo zoning a destinazione singola come Best practice per la configurazione dello zoning.

È necessario utilizzare Virtual Storage Console (VSC) per impostare policy di multipathing, perché imposta policy per tutti i dispositivi storage NetApp nuovi ed esistenti.

Errore host ESXi singolo



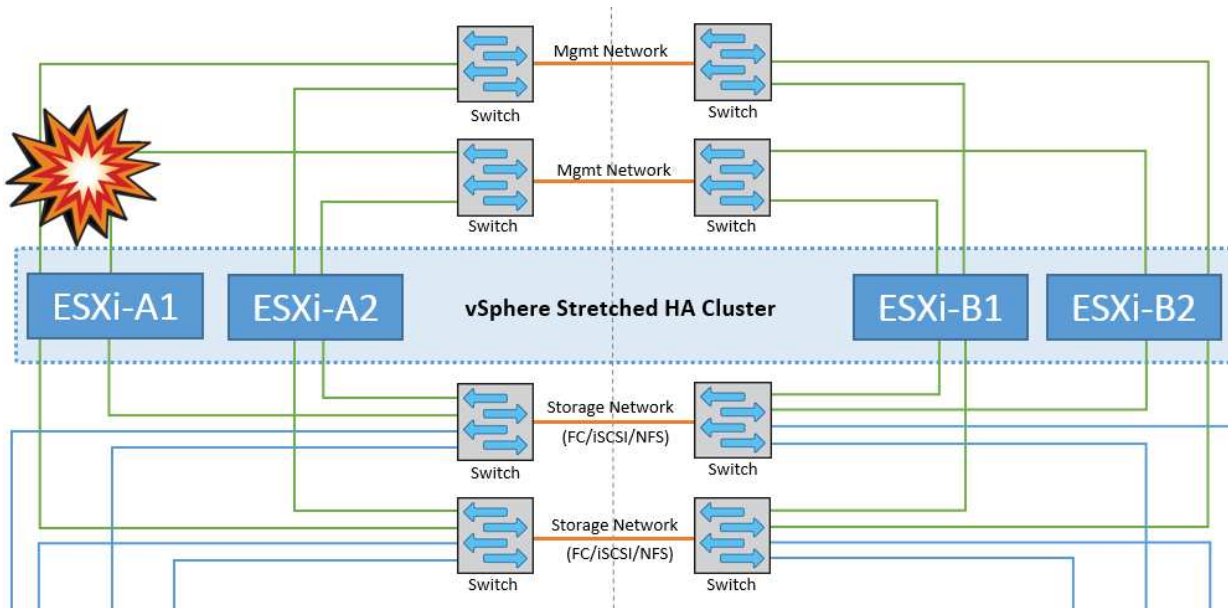
In questo scenario, se si verifica un guasto dell'host ESXi, il nodo master nel cluster VMware ha rilevato il guasto dell'host in quanto non riceve più gli heartbeat di rete. Per determinare se l'host è effettivamente inattivo o solo una partizione di rete, il nodo master monitora gli heartbeat del datastore e, se sono assenti, esegue un controllo finale eseguendo il ping degli indirizzi IP di gestione dell'host guasto. Se tutti questi controlli sono negativi, il nodo master dichiara l'host un host guasto e tutte le macchine virtuali in esecuzione su questo host guasto vengono riavviate sull'host rimasto nel cluster.

Se sono state configurate le regole di affinità per DRS VM e host (le VM nel gruppo VM sitea_VM devono eseguire gli host nel gruppo host sitea_hosts), il master ha controllato prima le risorse disponibili nel sito A. Se non ci sono host disponibili nel sito A, il master tenta di riavviare le VM sugli host nel sito B.

È possibile che le macchine virtuali vengano avviate sugli host ESXi nell'altro sito se è presente un vincolo di risorse nel sito locale. Tuttavia, le regole di affinità definite per DRS VM e host verranno corrette in caso di violazione di regole mediante la migrazione delle macchine virtuali a qualsiasi host ESXi rimasto nel sito locale. Nei casi in cui DRS è impostato su manuale, NetApp consiglia di richiamare DRS e applicare le raccomandazioni per correggere il posizionamento della macchina virtuale.

In questo scenario, non vi sono cambiamenti nel comportamento di MetroCluster e tutti i datastore continuano a essere intatti dai rispettivi siti.

Isolamento dell'host ESXi

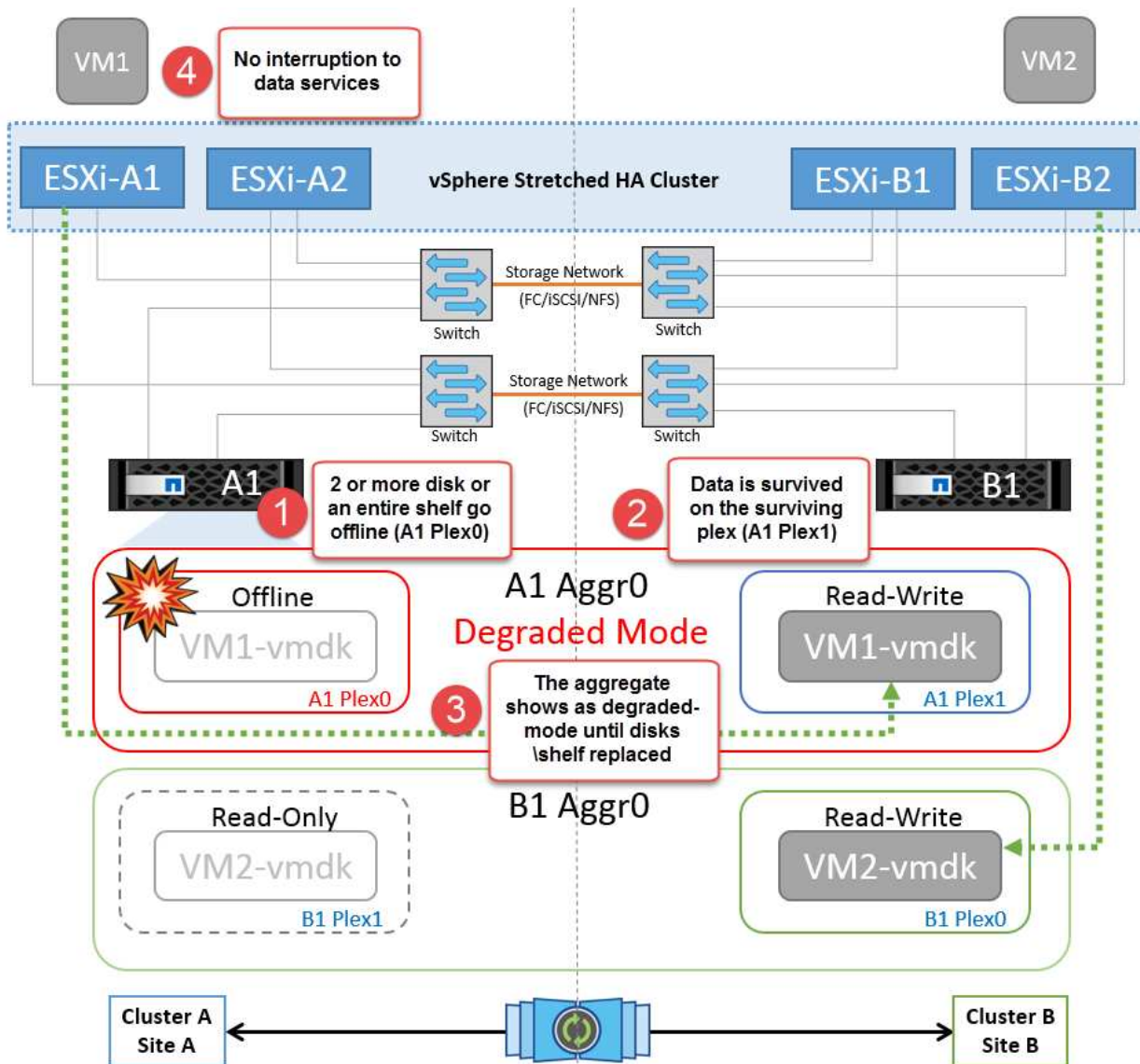


In questo scenario, se la rete di gestione dell'host ESXi non è attiva, il nodo master nel cluster non riceverà alcun heartbeat, pertanto l'host viene isolato nella rete. Per determinare se si è verificato un errore o se è solo isolato, il nodo master inizia a monitorare l'heartbeat del datastore. Se è presente, l'host viene dichiarato isolato dal nodo master. A seconda della risposta di isolamento configurata, l'host può scegliere di spegnere, spegnere le macchine virtuali o persino lasciare accese le macchine virtuali. L'intervallo predefinito per la risposta di isolamento è di 30 secondi.

In questo scenario, non vi sono cambiamenti nel comportamento di MetroCluster e tutti i datastore continuano a essere intatti dai rispettivi siti.

Guasto a shelf di dischi

In questo scenario, si verifica un errore di più di due dischi o di un intero shelf. I dati vengono distribuiti dal plesso restante senza alcuna interruzione dei servizi dati. Il guasto del disco potrebbe influire su un plesso locale o remoto. Gli aggregati vengono visualizzati come modalità degradata perché è attivo un solo plesso. Una volta sostituiti i dischi guasti, gli aggregati interessati si risincronizzano automaticamente per ricostruire i dati. Dopo la risincronizzazione, gli aggregati tornano automaticamente alla normale modalità con mirroring. Se più di due dischi all'interno di un singolo gruppo RAID si sono guastati, il plex deve essere ricostruito.

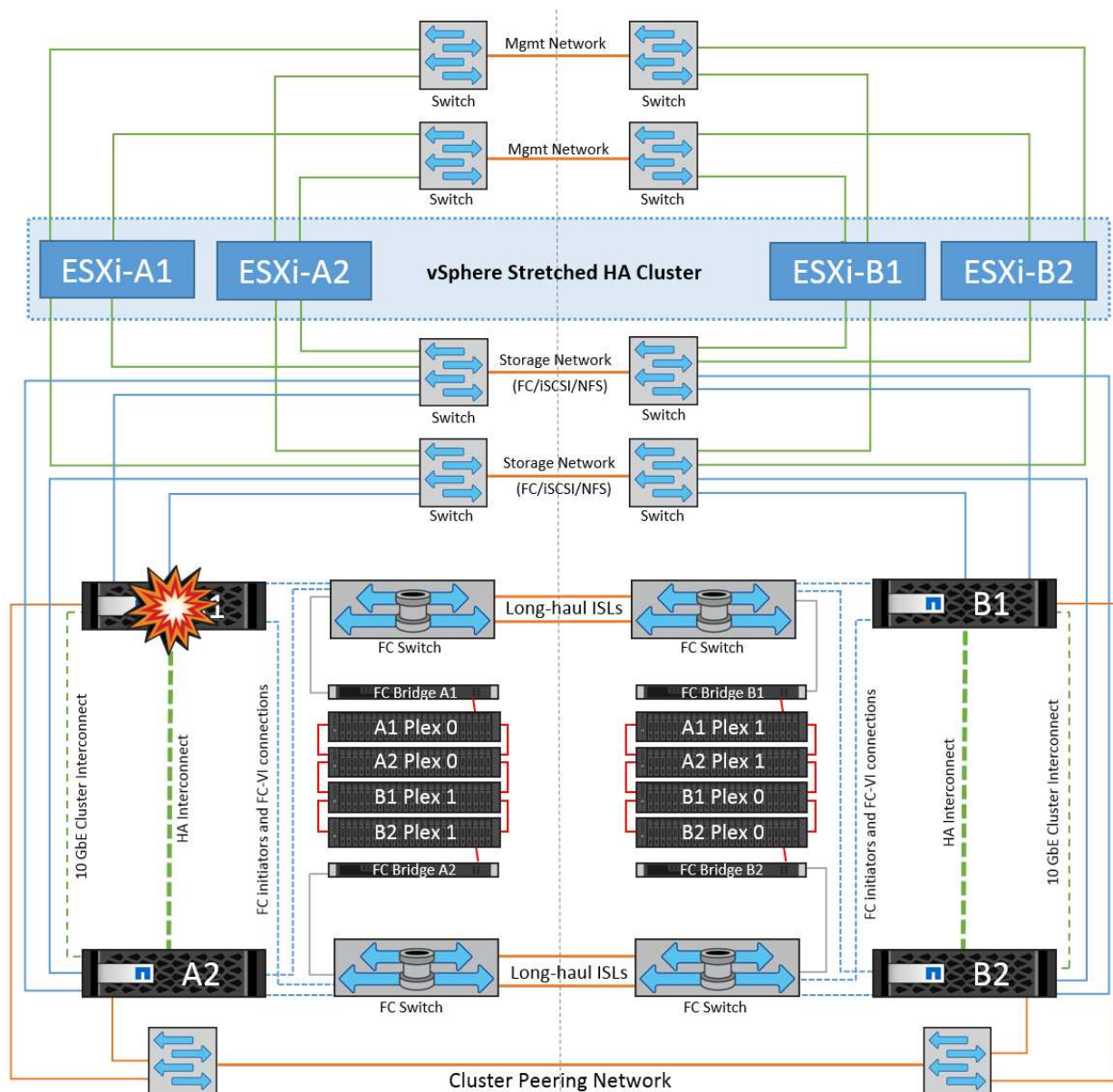


*[NOTA]

- Durante questo periodo, non si verifica alcun impatto sulle operazioni di i/o della macchina virtuale, tuttavia le performance sono peggiorate a causa dell'accesso ai dati dallo shelf di dischi remoto attraverso link ISL.

Guasto a un singolo storage controller

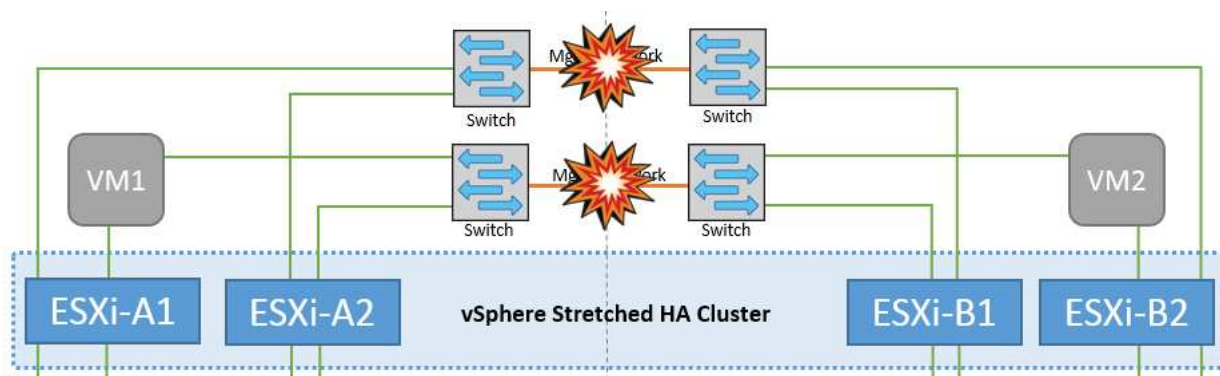
In questo scenario, uno dei due storage controller si guasta in un solo sito. Poiché è presente una coppia ha in ciascun sito, un guasto di un nodo attiva automaticamente il failover sull'altro nodo. Ad esempio, in caso di guasto al nodo A1, il relativo storage e carichi di lavoro vengono trasferiti automaticamente al nodo A2. Le macchine virtuali non saranno interessate perché tutti i plessi rimangono disponibili. I nodi del secondo sito (B1 e B2) non sono interessati. Inoltre, vSphere non intraprenderà alcuna azione perché il nodo master nel cluster riceverà comunque gli heartbeat di rete.



Se il failover fa parte di un rolling disaster (il nodo A1 esegue il failover su A2) e si verifica un successivo guasto di A2 o il guasto completo del sito A, è possibile eseguire lo switchover in seguito a un disastro nel sito B.

Errori del collegamento interswitch

Errore collegamento interswitch sulla rete di gestione

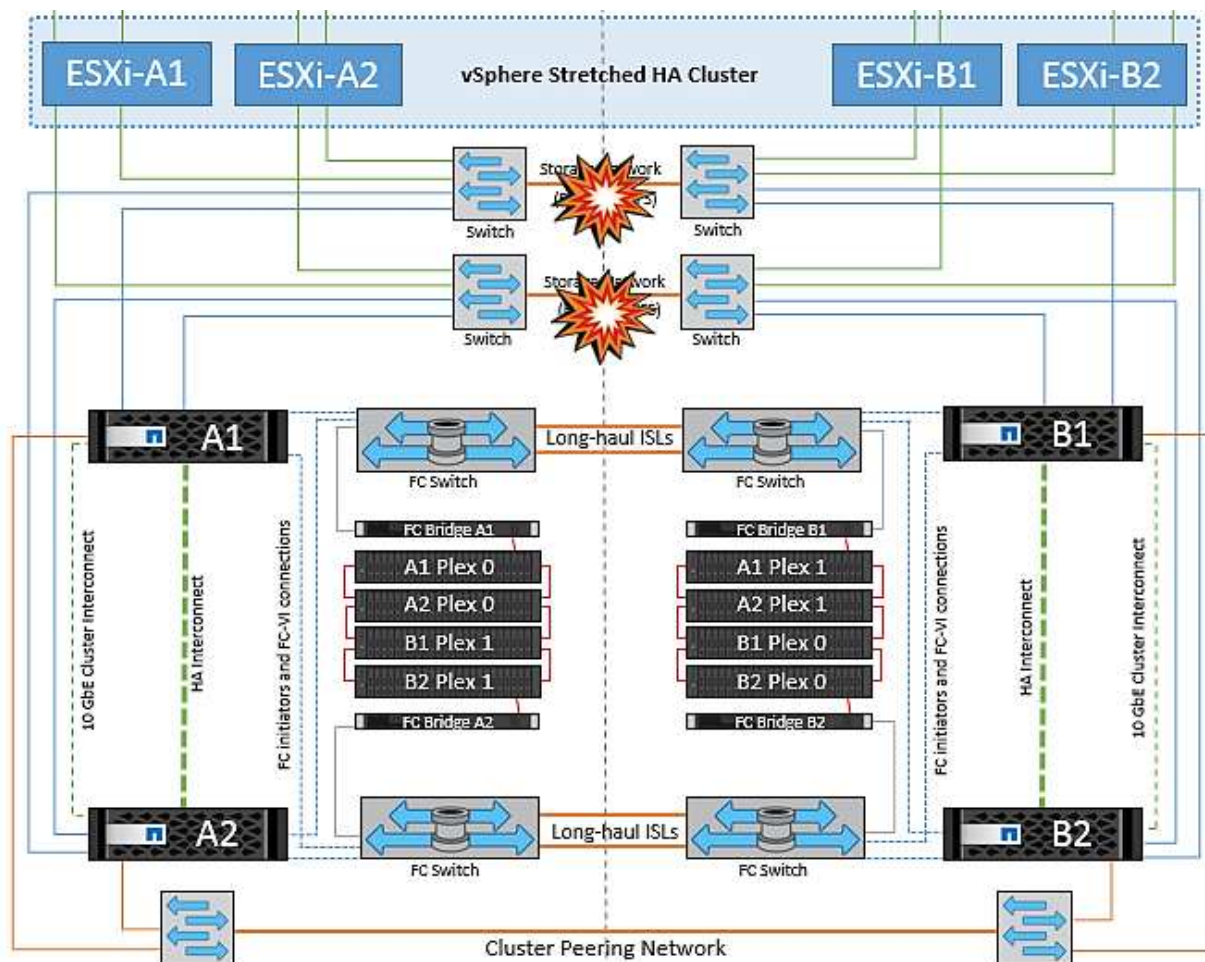


In questo scenario, se i collegamenti ISL nella rete di gestione host front-end si guastano, gli host ESXi nel sito A non saranno in grado di comunicare con gli host ESXi nel sito B. Ciò determina una partizione di rete poiché gli host ESXi in un determinato sito non sono in grado di inviare gli heartbeat di rete al nodo master nel cluster ha. Come tale, ci saranno due segmenti di rete a causa della partizione e vi sarà un nodo master in ogni segmento che proteggerà le VM da guasti host all'interno del sito specifico.



Durante questo periodo, le macchine virtuali rimangono in esecuzione e in questo scenario non si verifica alcuna modifica nel comportamento di MetroCluster. Tutti i datastore continuano a essere intatti dai rispettivi siti.

Errore collegamento interswitch sulla rete di storage

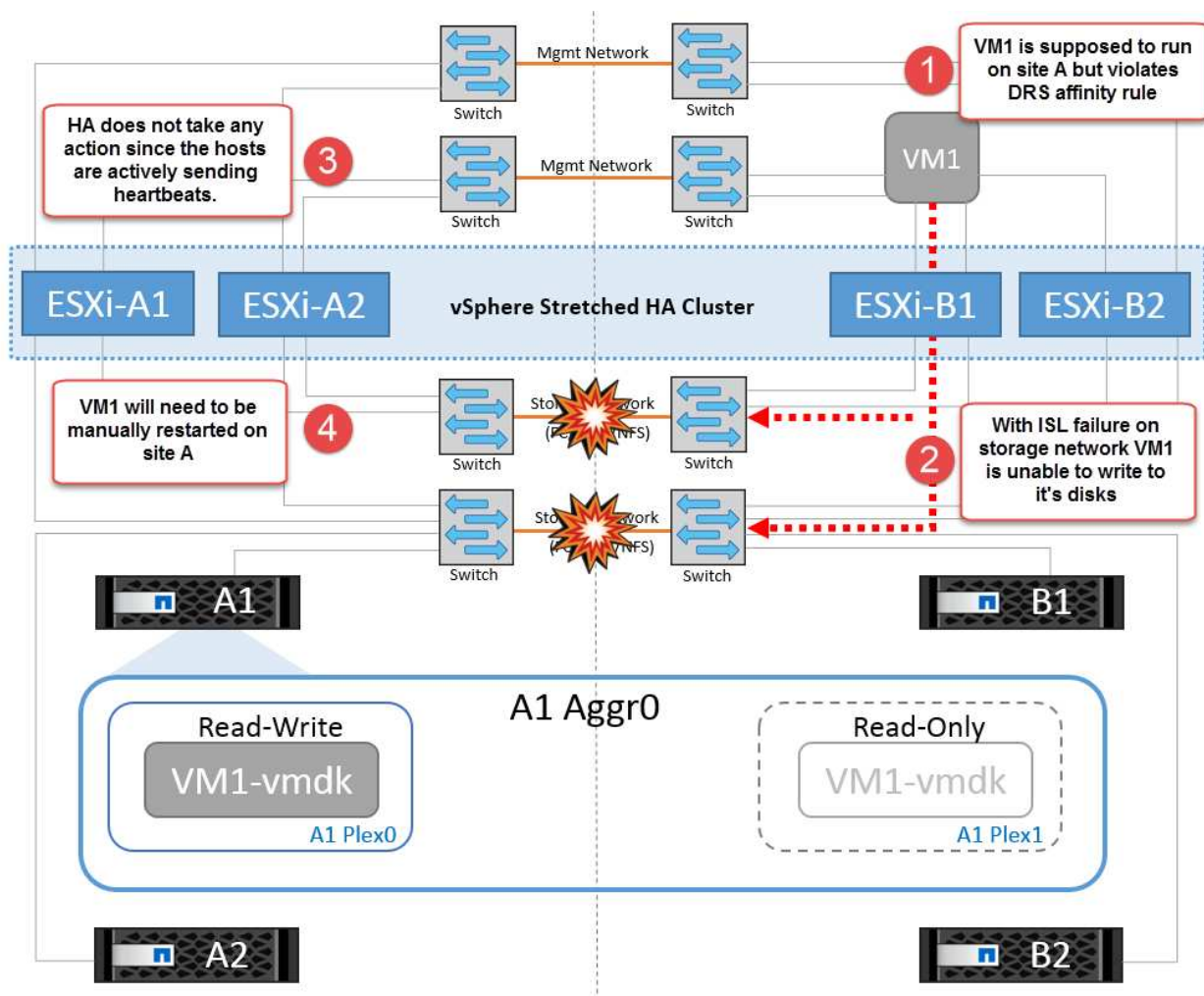


In questo scenario, se si verifica un errore nei collegamenti ISL nella rete di storage backend, gli host sul sito A

perderanno l'accesso ai volumi di storage o alle LUN del cluster B nel sito B e viceversa. Le regole VMware DRS sono definite in modo che l'affinità tra il sito host e il sito di storage faciliti l'esecuzione delle macchine virtuali senza impatti all'interno del sito.

Durante questo periodo, le macchine virtuali rimangono in esecuzione nei rispettivi siti e in questo scenario non si verifica alcuna modifica nel comportamento di MetroCluster. Tutti i datastore continuano a essere intatti dai rispettivi siti.

Se per qualche motivo è stata violata la regola di affinità (ad esempio VM1, che doveva essere eseguito dal sito A in cui i dischi risiedono sui nodi del cluster locale A vengono eseguiti su un host nel sito B), il disco della macchina virtuale può essere acceduto in remoto tramite i link ISL. A causa di un errore del collegamento ISL, VM1 in esecuzione nel sito B non sarebbe in grado di scrivere sui propri dischi perché i percorsi del volume di storage non sono attivi e quella particolare macchina virtuale non è attiva. In queste situazioni, VMware ha non intraprende alcuna azione poiché gli host stanno inviando heartbeat. Tali macchine virtuali devono essere spente e attivate manualmente nei rispettivi siti. La figura seguente illustra una VM che viola una regola di affinità DRS.

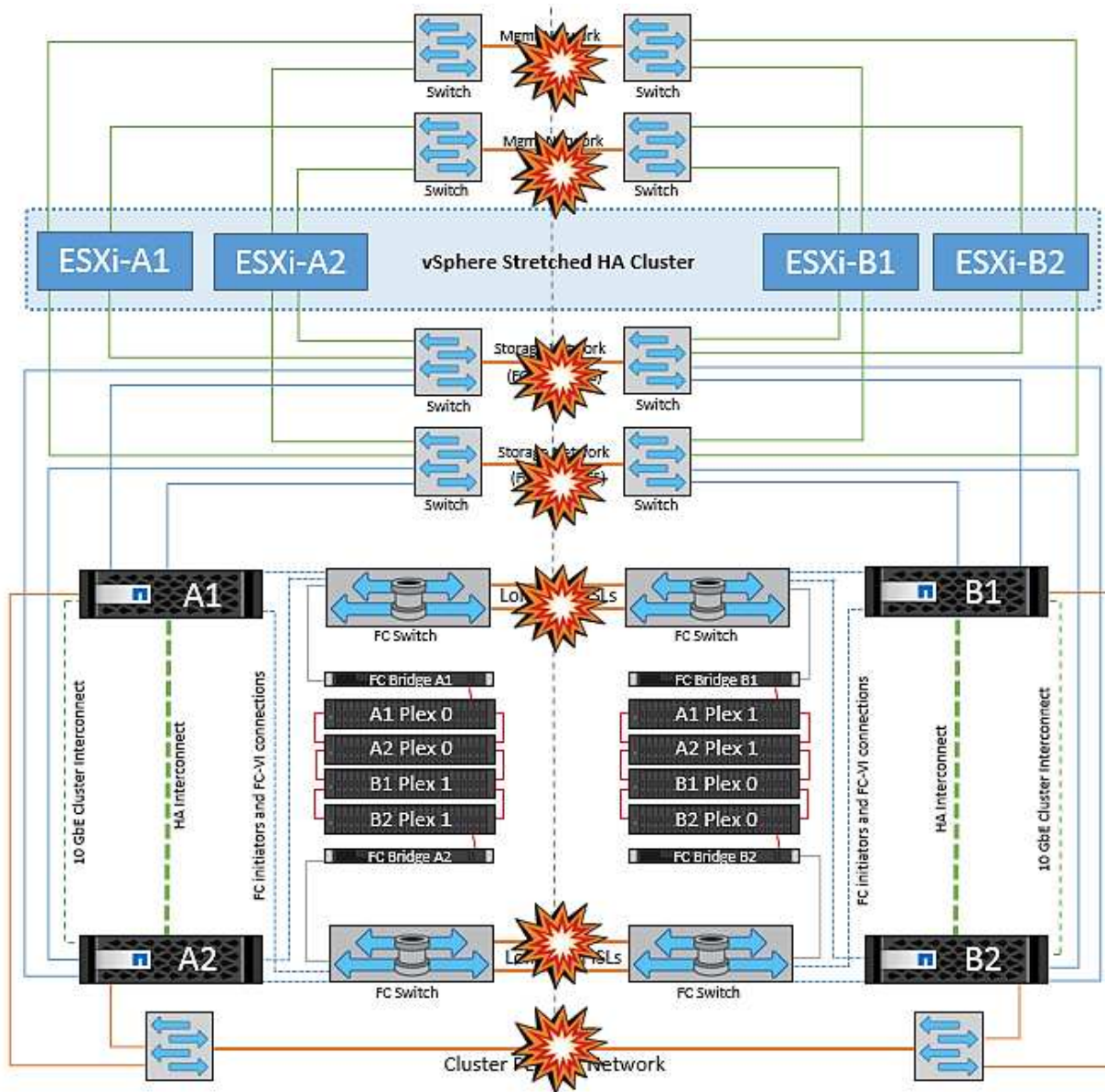


Guasto a tutti gli interswitch o partizione completa del data center

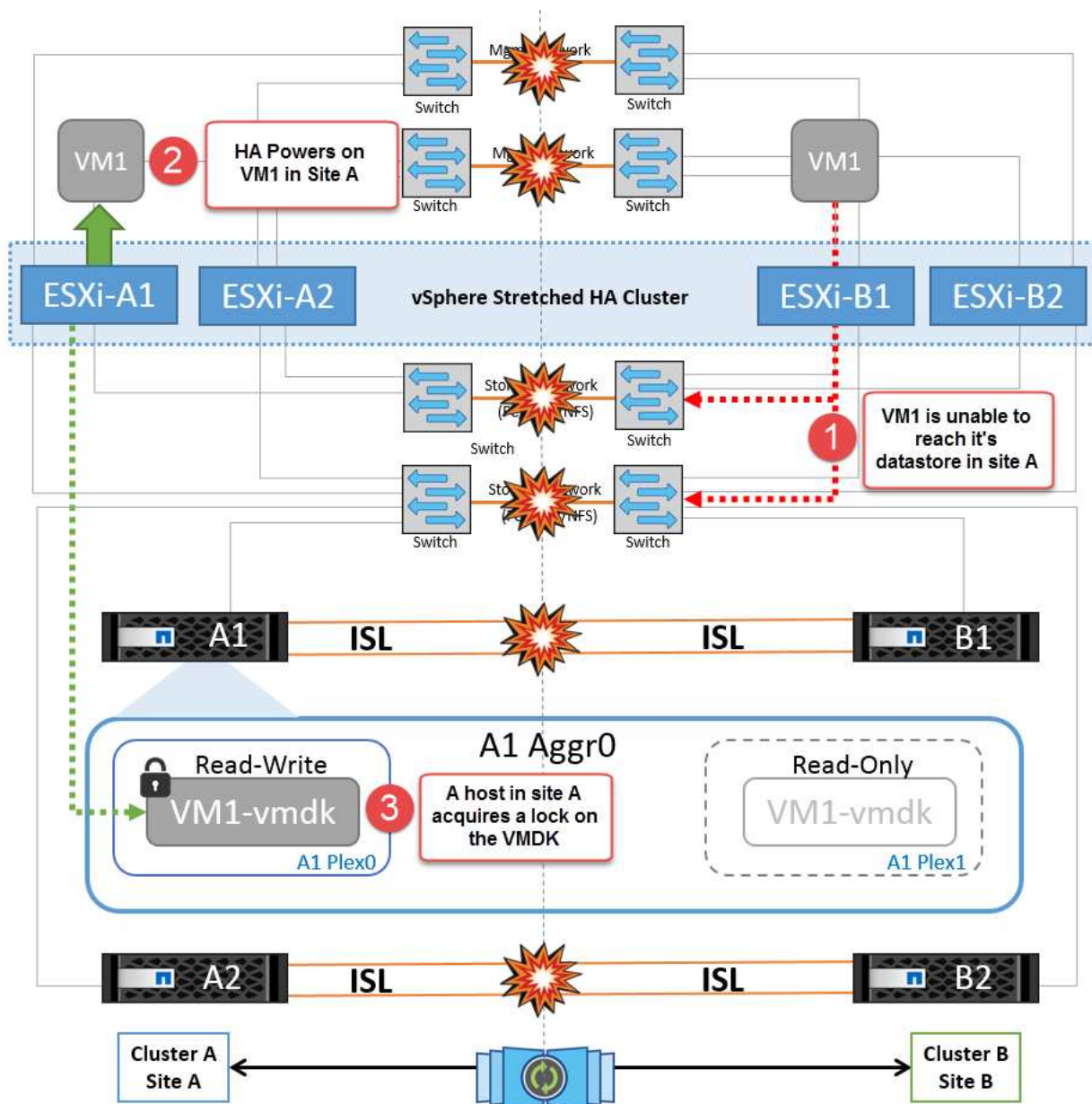
In questo scenario, tutti i collegamenti ISL tra i siti sono interrotti ed entrambi i siti sono isolati l'uno dall'altro. Come discusso in scenari precedenti, come ad esempio un errore ISL nella rete di gestione e nella rete di storage, le macchine virtuali non sono interessate da un errore ISL completo.

Dopo la partizione degli host ESXi tra i siti, l'agente vSphere ha controlla gli heartbeat del datastore e, in ciascun sito, gli host ESXi locali saranno in grado di aggiornare gli heartbeat del datastore nei rispettivi

volumi/LUN di lettura/scrittura. Gli host nel sito A supporteranno che gli altri host ESXi presenti nel sito B siano guasti a causa dell'assenza di heartbeat di rete/datastore. VSphere ha nel sito A tenterà di riavviare le macchine virtuali del sito B con un errore infine dovuto al fatto che i datastore del sito B non saranno accessibili a causa di un guasto all'ISL di storage. Una situazione simile si ripete nel sito B.



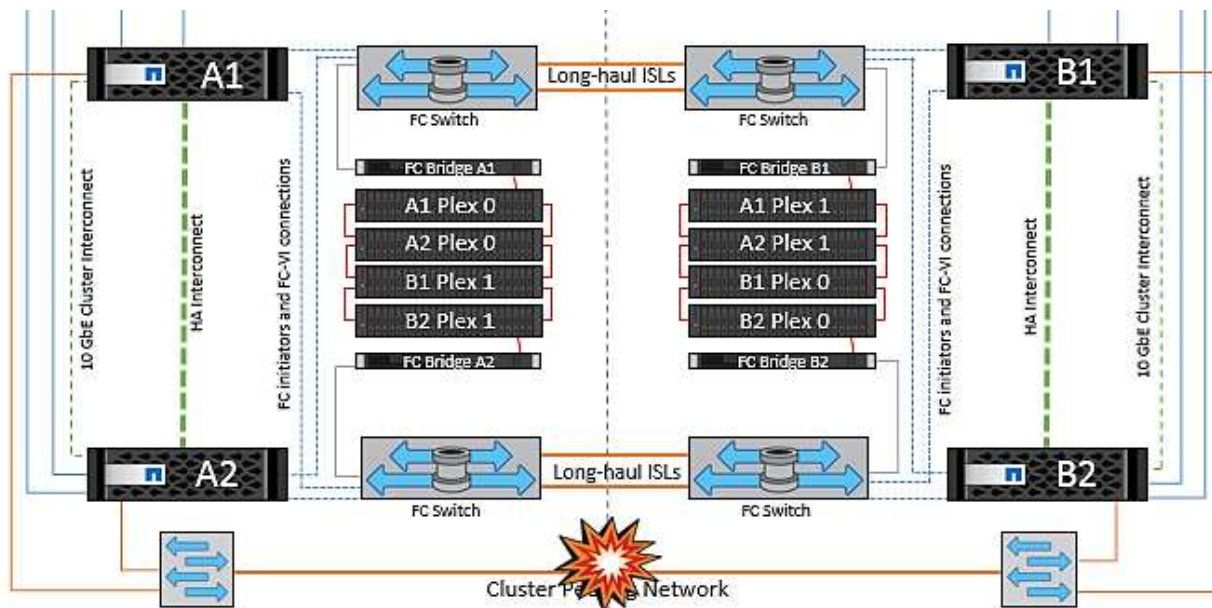
NetApp consiglia di determinare se una macchina virtuale ha violato le regole DRS. Tutte le macchine virtuali in esecuzione da un sito remoto non potranno accedere al datastore, quindi vSphere ha riavvia la macchina virtuale nel sito locale. Una volta che i collegamenti ISL sono tornati in linea, la macchina virtuale in esecuzione nel sito remoto verrà interrotta, poiché non possono esistere due istanze di macchine virtuali in esecuzione con gli stessi indirizzi MAC.



Errore collegamento interswitch su entrambi i fabric in NetApp MetroCluster

In uno scenario di errore di uno o più ISL, il traffico continua attraverso i collegamenti rimanenti. In caso di errore di tutti gli ISL su entrambi i fabric, in modo da eliminare un collegamento tra i siti per la replica di storage e NVRAM, ciascun controller continuerà a fornire i propri dati locali. Su un minimo di un ISL viene ripristinato, la risincronizzazione di tutti i plessi avviene automaticamente.

Eventuali scritture che si verificano dopo che tutti gli ISL sono inattivi non verranno mirrorate nell'altro sito. Uno switchover in caso di disastro, mentre la configurazione si trova in questo stato, causerebbe una perdita dei dati non sincronizzati. In questo caso, è necessario un intervento manuale per il ripristino dopo lo switchover. Se è probabile che non saranno disponibili ISL per un periodo prolungato, un amministratore può scegliere di arrestare tutti i servizi dati per evitare il rischio di perdita di dati se occorre eseguire uno switchover in caso di disastro. L'esecuzione di questa azione deve essere valutata rispetto alla probabilità che un evento disastroso richieda lo switchover prima che almeno un ISL diventi disponibile. In alternativa, in caso di errore degli ISL in uno scenario a cascata, un amministratore può attivare uno switchover pianificato verso uno dei siti prima che tutti i collegamenti abbiano avuto esito negativo.



Errore completo del sito

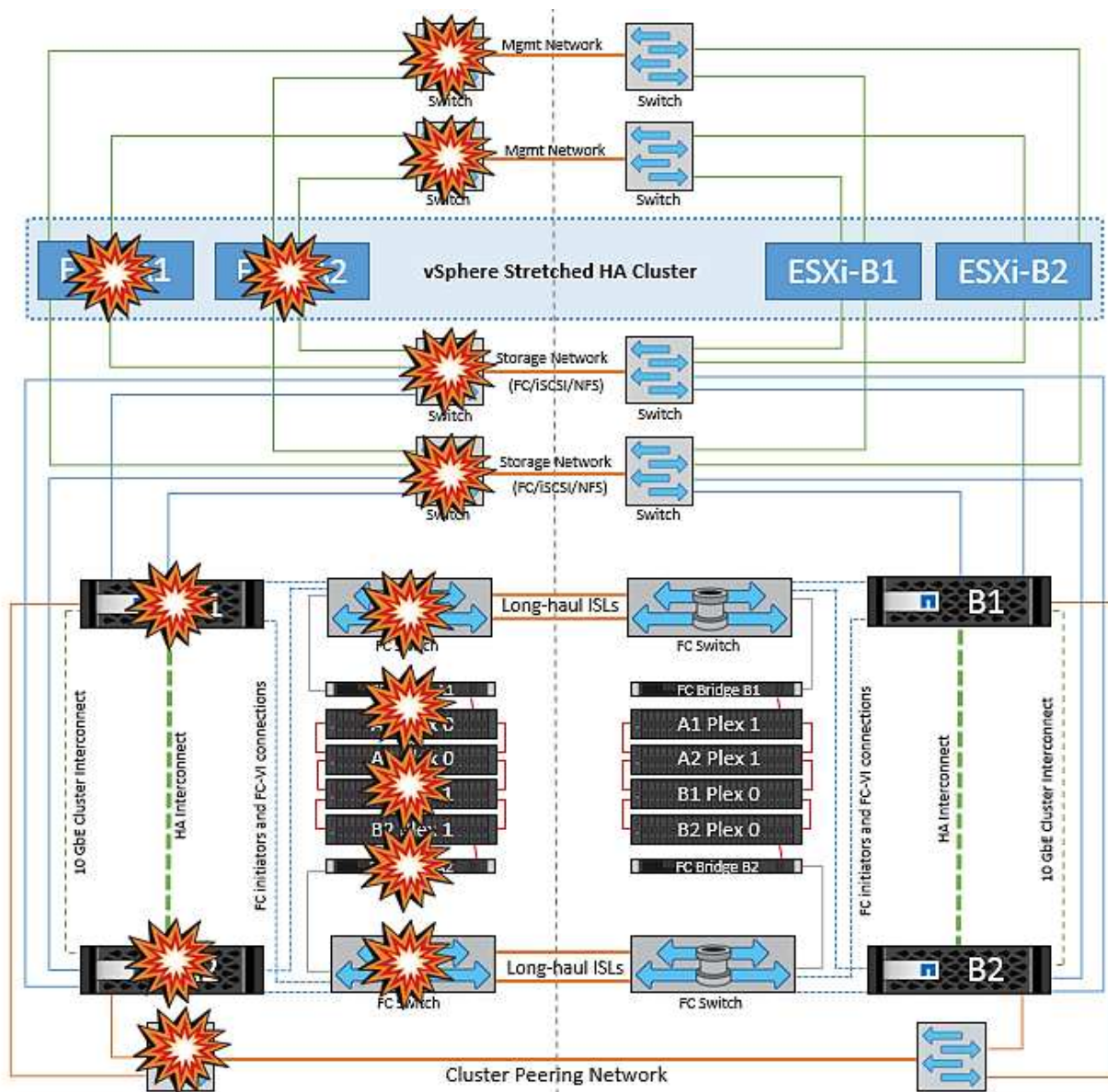
In uno scenario di guasto completo del sito A, gli host ESXi nel sito B non otterranno l'heartbeat di rete dagli host ESXi nel sito A perché non sono attivi. Il master ha nel sito B verificherà che gli heartbeat del datastore non siano presenti, dichiarerà che gli host nel sito A non sono riusciti e tenterà di riavviare le macchine virtuali del sito A nel sito B. Durante questo periodo, l'amministratore dello storage esegue uno switchover per riprendere i servizi dei nodi guasti del sito rimasto e ripristinare i servizi di storage del sito A del sito B. Dopo che i volumi o le LUN del sito A sono disponibili nel sito B, l'agente master ha tenterà di riavviare le macchine virtuali del sito A nel sito B.

Se il tentativo dell'agente master vSphere ha di riavviare una VM (che comporta la registrazione e l'accensione) non riesce, il riavvio viene rieseguito dopo un ritardo. Il ritardo tra i riavvii può essere configurato fino a un massimo di 30 minuti. VSphere ha tenta di riavviare il sistema per un numero massimo di tentativi (sei tentativi per impostazione predefinita).



Il master ha non avvia i tentativi di riavvio fino a quando il placement manager non trova lo storage appropriato, quindi in caso di un guasto completo del sito, ciò si verificherebbe dopo l'esecuzione dello switchover.

Se il sito A è stato sottoposto a switchover, un guasto successivo di uno dei nodi del sito B sopravvissuto può essere gestito senza problemi attraverso il failover verso il nodo rimasto. In questo caso, il lavoro di quattro nodi viene ora eseguito da un solo nodo. Il ripristino in questo caso consisterebbe nell'esecuzione di un giveback al nodo locale. Quindi, quando il sito A viene ripristinato, viene eseguita un'operazione di switchback per ripristinare il funzionamento regolare della configurazione.



Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.